Supply Chain Control Using a RFID Proxy Re-Signature Scheme

Trevor Burbridge, Andrea Soppera
BT Research, Ipswich, UK
{trevor.burbridge,andrea.2.soppera}@bt.com

Abstract—**The use of RFID tags allows many new approaches to the old problems of supply chain control and product anti-counterfeiting. Many of the schemes suggested to-date do not adequately meet the needs of the supply chain industry. Some require unjustifiable expense or performance and resilience issues, while others face deployment barriers where the party that deploys the technology is not the party the benefits. Many of the schemes, however, will ultimately fail because they inadequately address the issues of trust and business confidentiality. We present a supply chain control solution using the principle of proxy re-signatures to establish secure and verifiable supply chain paths. Critically our scheme does not require centralized run-time services and provides minimal visibility of supply chain operations to other parties.**

Keywords- RFID; Authentication; Supply Chain; Security

I. INTRODUCTION

Organisations are looking to their supply chains to tackle some of the most important business challenges today, from increasing sales to reducing time-to-market. Improvements in supply chain can yield benefits including:

- Increased supply chain velocity and market responsiveness
- Optimised inventory, enabling increased availability and stock turn while reducing safety stock levels and wastage of perishable goods
- Reduced shrinkage/theft, improved counterfeit and cost control
- Improved customer service by reducing errors and accelerating speed of response
- Real-time business information to identify areas for improvement
- Improved asset utilisation to reduce transport costs and minimised carbon footprint.

Many of these activities can be supported through the use of RFID to gather serial or item level information from the supply chain. In this paper we examine how RFID can be applied to protect supply chain operations. Many organizations are becoming increasingly interested in RFID-based supply chain security, either because they see it as a dominant business justification for the introduction of RFID (for example to restrict counterfeit operations) or because they have already deployed RFID and are looking to stretch the business value they can achieve from their deployment.

Despite many alternative RFID authentication and supply chain security schemes being proposed, there is little agreement in industry on the best technology to adopt. Part of the reason for this is that no scheme is clearly better; rather they have different properties that may be suited to different uses. In section II we explore some of these alternative RFID approaches to product authentication and supply chain control. In section III we state our objectives for improving on these current systems, and our broad approach in IV. We continue to present our design by outlining a number of technical options in V and elaborating on our chosen option in VI. In part VII we consider how an attacker may attempt to defeat the system, and revisit our design goals in VIII before finally concluding the paper.

II. AUTHENTICATION AND SUPPLY CHAIN CONTROL

The uncertain security of proprietary 'lightweight' security schemes has started to give way to standards-based cryptography (e.g. AES) [1] and Physical Unclonable Functions (PUFs) [2]. Such schemes allow authentication of the RFID tag since the cost to clone such a tag is infeasible for most applications. Any successful attack is limited since the secret used is unique to each tag. The disadvantage of such schemes is that the cost of each tag is increased and that a network of authentication servers must be deployed to hold the tag secrets securely and participate in the tag challenge-response. Aside from the costs of such infrastructure and the problem of reliance on such external systems, the authentication servers may also gain visibility of the supply chain operations. A future move to asymmetric cryptography (e.g. ECC) [3][4] would allow authentication to be performed locally using a public key. The other point to note is that tag authentication is not product authentication and to use one for the other relies on the secure binding of the tag to the object.

Authentication, however, is not the only security concern within supply chains. Manufacturers also often desire to control the route to market of their products and to stop grey market trading. Reasons for this may be purely economic, or may be motivated by the correct care of their goods and customers. Product authentication alone does nothing to address these problems. Track and trace solutions [5] can provide supply chain visibility and hence control. If the route to market can be authenticated, then the product is also

978-1-4244-5743-4/10/$26.00 ©2010 IEEE

authenticated at the same time. Any such approach relies upon the quantity and the quality of the track and trace information. Supply chain participants must be motivated to share their product visibility information; an operation which is not without cost or risk to their own business confidentiality. Also the integrity of the information must be assured to stop malicious parties from corrupting the track and trace information (and thus hiding their malicious operations). One option to improve the integrity of the information is to use authentication capable RFID tags and trusted RFID readers [6][7][8] (to ensure that the right goods have been read at the right locations). Such an approach also provides defence-in-depth against counterfeiting, since an attacker would need to clone the RFID tag and also counterfeit a plausible product history in the track and trace systems.

A final class of solution is to build up some supply chain history or pedigree along with the flow of the physical goods. Such information may be accumulated in electronic (or even paper) documents, or with the increasing memory capacity of RFID tags, may be written into the tag user memory. Such trace information must be digitally signed to prevent an attacker inventing product history. Usually trace information is appended to the history information. This allows any part of the history to be independently verified. Alternatively the previous signature may be over-signed. This approach saves memory but relies on all public keys being available to the end verifier in order to 'unpeel' the product history. It does, however, bind the complete trace history together so that records cannot subsequently be added or removed. Multi-signature schemes allow multiple parties to create a joint signature that may have fixed length [9]. An alternative suggestion has been to use write-only memory in the tag. One problem with such approaches is that a genuine trace history may be cloned. The incorporation of the unique product code in the signature prevents an attacker from claiming the history for another item, but does not stop them cloning the identifier for a counterfeit product. Although such duplicates may be detected using a central system, this may not be sufficient in supply chains where prevention is required (such as where human safety is impacted). Reliance of a unique Tag Identifier (TID) to prevent transfer onto another tag has been shown to be a dangerous assumption [10], so combination with secure authentication capable tags should be considered. A final problem with such an approach is that any downstream party gains full visibility of the upstream supply chain. This information is often considered to be confidential since it can be used by competitors in the supply chain.

III. DESIGN GOALS

In this paper we attempt to design an RFID-based supply chain security solution that mitigates some of the problems with existing schemes and thus is more widely applicable. In this section we outline the goals we have tried to achieve, which we revisit later in the paper.

A. Limited supply chain visibility

The universal failing of all of the schemes in the previous section (with the exception of tags capable of asymmetric cryptography) is the leakage of supply chain operational data that may be considered confidential. Such leaks can occur where supply chain information is shared to a central authority or along the supply chain, but can also occur during the authentication or supply chain verification process as well. Our major motivation in writing this paper is to present a scheme in which supply chain information is at most shared between adjacent peers in the supply chain. Thus, for example, a retailer may not be able to determine the logistical partners chosen by the manufacturer. Neither will a supply chain service have access to volume information for certain products.

B. No central run-time authority

We desire that the scheme should be able to operate without a central authority. Aside from the visibility issues discussed in (A), use of a central authority impacts on the performance and resilience of supply chain operations. For example, what happens when goods cannot be authenticated because the central authority is unreachable? Also for political and confidentiality reasons such an authority may not be selectable. Of course, some authorities are in fact necessary to establish the rules for the correct operation of the supply chain, but such involvement should be kept to policy dissemination and reporting of violations.

C. Applicable to cheap insecure tags

Many of the schemes already discussed suffer from weaknesses if secure cryptographic tags are not employed. We attempt to design a scheme that is applicable to cheap insecure tags such as EPC Gen2.

D. Supply chain control

We attempt to solve the wider problem of supply chain control instead of just providing an anti-counterfeiting solution. If the route to market can be adequately controlled it can be used to prevent counterfeits, but also to control grey markets and maintain the quality of goods and customer service by only using authorised (e.g. approved, trained and/or certified) handlers.

IV. OVERALL APPROACH

Current pedigree or supply chain history approaches fail to meet many application requirements due to the visibility of supply chain information to downstream parties. The same information that is used to check the veracity of the supply chain route can be used to analyse and undermine competitors. In addition the checks are often performed only at the end of the delivery cycle. Technically this requires knowledge of the public keys of every party in the supply chain. Operationally it means that any imagined discrepancy must be checked against the actual business arrangements and contracts for each party.

We believe significant benefits might be achieved if instead

of an end-to-end approach, the supply chain is checked at every path segment between participating supply chain players. If the path can be verified at each hop, then the upstream history can be discarded. Instead of each partner verifying the entire path, they verify the path only from the previous trusted party. In such a manner a chain of trust is established between the supply chain verifier and the start of controlled path (e.g. the manufacturer).

Technically such a scheme might be naïvely implemented by splitting the overall supply chain policy into permitted segments. These segment policies are then distributed to the receiving party for each segment. When goods arrive the receiving party will then check a tag signature to confirm the segment shipping party and also check their local policy to see whether they are allowed to receive goods from that party.

Such a naïve scheme does stop untrusted parties from injecting goods into the supply chain since they will not be trusted to act as a shipper for a controlled supply chain segment. However the problem becomes a balance between the level of trust in each supply chain party and the degree of control that is required in the supply chain. If only the most trusted parties participate, then the supply chain has only few verified segments. Violations occurring within a segment (e.g. goods being lost or introduced) are hard to pinpoint to a single party. Also with too few participating parties it may be impossible to enforce certain policies (such as keeping goods within certain countries). Conversely, if the level of trust required is lowered then many more parties are available to participate in the scheme. While granular control of the supply chain is possible, the integrity of the scheme may be undermined. Authorised shippers for a segment may pretend that they have checked an upstream leg (without doing so since this is a cost to themselves) or may even introduce counterfeit goods, signing to say that the goods have followed a legitimate path from the correct manufacturer. If such goods are later discovered to be counterfeit, it would be impossible to detect who first signed the goods unless detailed receiving records are kept for each segment. Even for a limited detection time window this may be prohibitive. Thus, although the approach sounds attractive it is marred by several problems.

Our approach builds on this naïve implementation by ensuring that a segment shipper can only sign goods that have followed an authorised upstream segment. Thus, any supply chain party, no matter how untrustworthy, may act as a receiver/shipper for the supply chain segments.

V. Options For Secure Re-Signing

We have considered three methods for ensuring that untrusted parties may act to verify the upstream supply segment and generate new tag signatures. We outline all three approaches, although we only develop our preferred option within this paper.

A. Trusted Re-Signing Service

One simple solution to the problem of untrusted parties acting within our system is to remove the critical operation into a trusted service provider. Although the untrusted party is allowed to act as the receiver and shipper of goods within the supply chain model, they are not allowed to produce the tag signature themselves. On receiving goods the untrusted party will check the identity of the goods, the identity of the upstream shipper and the receiving policy that they have been given in advance. This policy is then used to identify a Trusted Re-Signing Service (TRS). The scheme allows multiple manufacturers or other supply chain authorities to choose their own TRS operator.

The supply chain party sends the previous signature and product identifier to the TRS. The TRS validates the upstream path segment before issuing a new signature to the supply chain party. The supply chain party writes the new signature onto the tag before shipping the goods onwards towards authorised receivers.

This alternative is not preferred since the routine operation of the supply chain requires communication with the TRS, breaking our goal of having no central run-time authority. The use of the TRS could impact the performance and resilience of supply chain operations.

B. Trusted Re-Signing Apparatus

If secure system operation is required within the domain of an untrusted party, a well established method is to secure an island within the untrusted domain on which the critical operation is performed. Such an island can be established by using a Trusted Platform Module (TPM) [11]. Other work, for example, has shown how a Trusted RFID Reader can be designed that incorporates such a TPM [6][7]. A resigning service could operate locally on such a trusted reader, or on another trusted computing platform. We call such a re-signing platform a Trusted Re-Signing Apparatus (TRA). The supply chain authority can check the integrity of the TRA remotely to ensure that its operation has not been corrupted. The use of the TPM also allows the re-signing keys to be securely stored so that any breach of the TRA will not release such keys. The resigning keys are instead only available to the local re-signing service, and the resigning service will only run if the rest of the TRA passes its integrity check.

This option meets our design goals and has been elaborated and reported within a deliverable of the EU BRIDGE project [8]. The use of the TRA has both advantages and disadvantages. The deployment of a complete apparatus means that it can easily be installed behind any standards compliant reader (e.g. EPCglobal RP) or RFID event processing interface (e.g. EPCglobal ALE) without further integration. Only an internet connection to the supply chain authority to receive policies and keys and to report violations is required. The disadvantage of such a system is the costs of producing and installing the apparatus, along with checking and maintaining its integrity.

C. Proxy Re-Signatures

The third alternative to securing the upstream verification and re-signing operation is to use a proxy re-signature technique [12][13].

A proxy re-signature is a primitive where a proxy (in our case the supply chain partner) is given some information which allows the transforming of Alice's signature (in our case the upstream shipper) into Bob's signature (in our case the receiver's signature). However, the proxy does not control the private key associated with Alice or Bob and therefore it cannot directly generate the signature for either Alice or Bob.

The proxy translates a perfectly-valid and public-verifiable signature from Alice into one from Bob. Given a message *m* and a signature of the message with Alice's private key, $\sigma_{A(m)}$ the proxy can convert it into a valid signature from Bob $\sigma_{B(m)}$. A property of *multi-use* proxy re-signature is that the "translation" from one signature to another can be performed in sequence and multiple times by distinct proxies without requiring the intervention of the signing entities (the owners of the private keys). In this way, the private keys can always remain offline and protected. All the signatures are publicly verifiable signatures as if they were signed by the real owner of the distinct entities.

Ideally we desire a proxy re-signature scheme that it is uni-directional and transparent. The property of uni-directional means that the proxy can only translate signatures one direction. This means that the supply chain party cannot receive goods from the upstream shipper, translate the signature to its own, and then translate it again to a different upstream shipper from which it is also permitted to receive goods. Although most multi-use schemes to date are theoretically bi-directional, in practice they can be made into a uni-directional scheme through the controlled distribution of the cryptographic keys [13], which is achievable in our design. A uni-directional scheme has been proposed [14] but suffers from the linear growth of the signature which makes it unsuitable for limited memory RFID applications. The property of transparency means that any observer cannot tell that any translation has taken place. Thus to each downstream receiver it looks as if the upstream shipper has created the signature. The receiver (or any eavesdropper) cannot determine any information upstream of the shipper for the path segment. Thus proxy re-signatures look at first glance to be an excellent technique to secure a supply chain path without leaking information along the supply chain. In the rest of the paper we refer to the re-signing proxy as an RP.

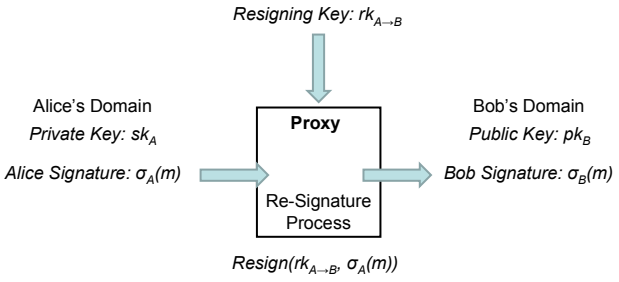

Figure 1. Proxy Re-signature Operation

VI. Applying Proxy Re-Signatures to Supply Chain Control

Every party that wishes to exercise control of path segments between the participating supply chain parties will act as or use a Supply Chain Controller (SCC). The SCC maintains a model of the supply chain graph for the limited set of goods over which it wishes to exercise control. Directed edges in the graph are labeled with the item identifiers that are permitted to flow along them (by that controller). The use of structured item identifiers such as EPCglobal EPCs (e.g. an SGTIN) [15] allow wildcard templates to be used to succinctly describe sets of goods such as product types or batches. Selected nodes in the graph are designated as being permitted to introduce selected goods (again using item identifier wildcards) into the supply graph. The graph can be either acyclic or may also allow the return of goods. A bi-directional proxy re-signature scheme [13] is not necessary since nodes can be assigned multiple private keys (i.e. the return path is simply modeled as an onward path to a new node for the same organization). The SCC will generate one or more private/ public key pairs for each node in the graph that has children. Nodes without children represent final receivers in the supply chain that do not need to sign goods. The SCC also generates a resigning key for each directed edge in the graph, which represents a supply chain segment. This resigning key would normally be given to the proxy in a proxy re-signature scheme and translates a signature by the key associated with the parent node to a signature by the key associated with the child node. In our case it will be used by each node in the supply chain graph to translate the signature of the previous shipper to the signature of the shipper for the next path segment (synonymous with the receiver of the previous segment).

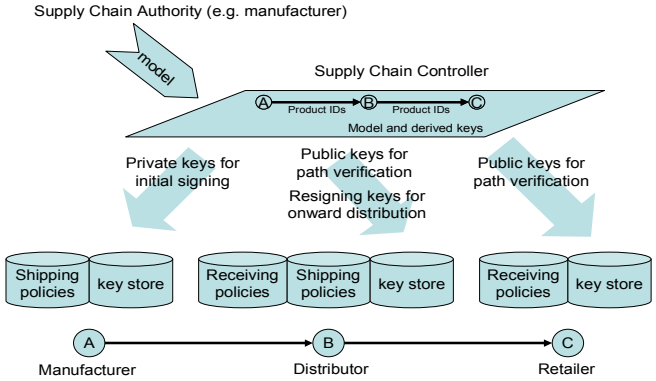

Figure 2. The role of the Supply Chain Controller in generating and distributing policies and keys

Once the public/private and resigning keys have been generated, the keys are distributed to the supply chain partners that operate the supply chain graph nodes. Private keys are only given to nodes that are allowed to introduce goods (e.g. manufacturers). Any partner with a node capable of receiving goods (i.e. any node with a parent in the graph) is given the set of public keys associated with the goods on incoming edges. In addition any node capable of both receiving and shipping goods is given a set of resigning keys. We will discuss the

number of private and resigning keys later in this section.

The supply chain participants fall into four categories, only the first of which is disjoint from the others.

A) Partners which do not participate in the scheme and are not represented in the graph
B) Partners which are able to introduce goods into the supply chain
C) Partners who are able to ship goods onwards
D) Partners which are able to verify that a legitimate path has been followed

Partners in category (A) are of little concern to our technical scheme and are simply 'tunneled across' (i.e. they transport the goods with signatures). Manufacturers of goods would normally fall into category (B). However, it is also possible to imagine supply chain partners that are able to both introduce and re-ship goods, thus performing roles (B) , (C) and (D) (e.g. a packaging company that receives only a subset of goods with pre-attached RFID tags). Intermediate parties in the supply chain will normally perform roles (C) and (D), whereas final receivers will perform role (D). These roles match closely with the keys that they receive from the SCC and the process steps which they operate using the keys.

We define three processes that each party may operate:

A. Signature creation

Parties that introduce goods into the controlled supply chain graph receive one or more private keys from the SCC. The keys are transmitted using a secure communication channel and must be stored securely by each party. Each party also receives a signing policy which specifies which key (if given more than one) to use to sign the tags of which goods. Before shipping the goods the signature creator will read the unique item identifier (e.g. EPC) and TID if used and create the signature $\sigma_A(EPC, TID)$ where σ_A is a signature performed with the private key sk_A. They will then write the signature into the user memory of the tag along with a key-pair identifier that was supplied by the SCC along with the private key.

B. Verification

Parties that receive goods (including intermediate supply chain partners and final receivers) must perform a verification step on any received goods.

The receiver reads the EPC and TID from the tag along with the signature and the key-pair identifier. The receiver then checks its receiving policy (distributed by the SCC) for the key-pair identifier. If the key pair identifier is not in the receiving policy then the receiver is not authorised to receive the goods. This may be because the goods have been shipped in error. If the key-pair identifier is found then the public key (transmitted from the SCC as part of the receiving policy) is used to verify the tag signature. If the signature is correct then the receiver is allowed to receive the goods. If the signature fails then either the shipper has failed to sign the goods correctly or a malicious party is attempting to introduce goods.

C. Re-signing

An intermediate supply chain partner should only proceed onto the re-signing process after a successful verification process has been completed. Goods which fail the verification process should be alerted to the SCC. An attempt to re-sign goods which have failed verification will result in a signature which is not verified by the next partner in the supply chain.

The supply chain partner will have received a shipping policy from the SCC. This policy specifies which resigning keys (rk_i) should be used against which goods. The re-signer retrieves the resigning key from the key store populated by the SCC) and performs the proxy re-signature operation using the resigning key. It also retrieves the key-pair identifier received in conjunction with the resigning key and writes both the signature and the key-pair identifier to the tag, overwriting any previous tag data.

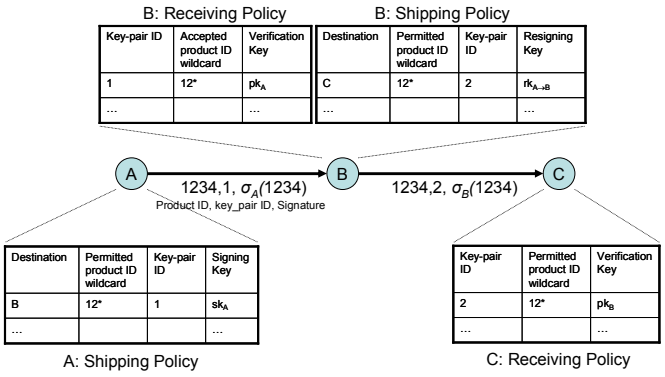

Figure 3. Example receiving and shipping policies

The Use of Multiple Node Keys

Previously it has been mentioned that multiple key-pairs can be associated with a node in the supply chain graph. This allows different goods to be signed with different keys, ensuring that specific goods follow divergent paths later in the supply chain. For example, in Figure 4 goods signed $\sigma_{A1}(EPC, TID)$ will flow to partner C, whereas goods signed $\sigma_{A2}(EPC, TID)$ will flow to partner D. C will only verify goods signed σ_{B1} and D will only verify goods signed σ_{B2}.

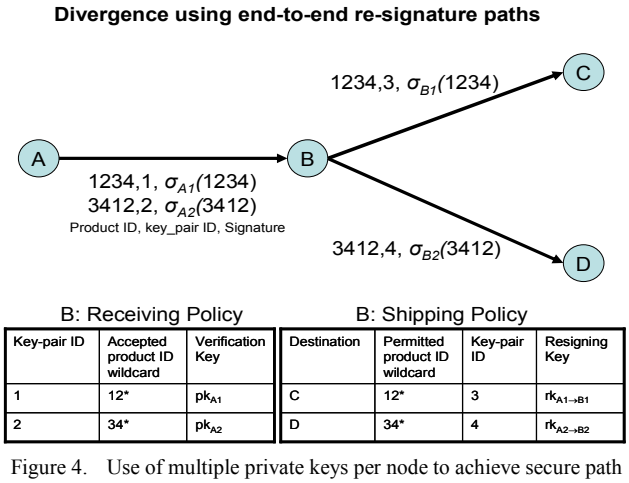

Figure 4. Use of multiple private keys per node to achieve secure path divergence

In the intermediate supply chain such behaviour cannot be

achieved securely by B using two resigning keys $rk_{A\rightarrow B1}$ and $rk_{A\rightarrow B2}$ that are applied to the same signature from A. B would have to apply the correct resigning key specified in the shipping policy for the goods to be accepted by each of its downstream partners, but would be free to allocate goods how it wanted to each path segment. Thus, if the splitting of goods is to be constrained later in the supply chain, the signature splitting must take place earlier by a trusted supply chain partner, or even by the manufacturer at the start of the supply chain graph. Fortunately, if the physical divergence of goods is specified in the SCC supply chain model, the SCC can automatically generate the multiple signing (private), resigning and verification (public) keys that are required.

D. A Simpler Approach to Divergent Paths

An alternative to signature splitting is to rely on the receiver policy. This policy can be extended to specify which goods may be accepted from which shippers. If the shipper breaks their shipping policy by sending the goods the wrong way then this will violate the receiver policy. The weakness of this approach is that a number of intermediate parties may collude to ignore their shipping and receiving policies providing that the goods converge again later in the supply chain (with the same signature). Since it is unlikely that many supply chain authorities will care about controlling the separation of goods if they are subsequently re-merged, then this approach is reasonable, simpler to understand and results in smaller policy tables and key stores (since each partner only has one shipping signature requiring N resigning keys where N is the number of upstream shippers from which it receives goods).

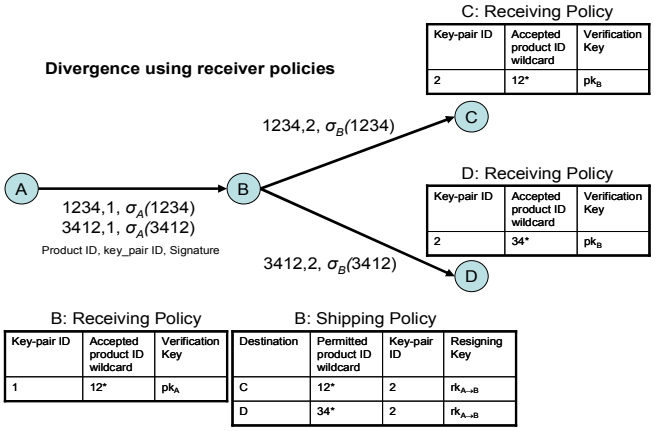

Figure 5. Using receiver policies to avoid the requirement for end-to-end res-signature paths

E. Dynamic Supply Chains

The scheme allows the SCC supply chain model to be dynamically updated. The SCC creates the new policies and keys and transmits then to the supply chain operators. If the simpler approach to product divergence is used then this has little impact on the supply chain operation. Nodes will receive new shipping and receiving policies only if their physical operations also change (e.g. shipping different goods to different receivers). New keys are only required if a new upstream shipper is introduced for that receiver. The introduction of policies should be managed to ensure that goods shipped according to policy do not fall foul of a newly introduced receiving policy (while they were in transit). Thus previous receiving policies may be operated in parallel with the new receiving policy for a limited time.

If the more complex goods divergence scheme is used then even a simple change late in the supply chain may necessitate new keys and policies being sent to the upstream supply chain partners.

VII. ATTACK MODEL

We consider three categories of attacks on the supply chain, namely the introduction, removal and substitution of goods. We also briefly consider attacks on the scheme itself.

A. Goods Introduction

The motivation for introducing goods into a supply chain may be to introduce counterfeit goods or re-introduce genuine goods from which the tag and hence supply chain validation has been removed. Such introduction may also occur when goods have followed an illicit path and re-injected back into the permitted supply chain.

In all these cases the attacker may attempt to produce a valid signature of a permitted upstream shipper before passing the goods to the receiver in the authorised supply chain path. Assuming that physical location is of no concern to the attacker it can attempt to produce the signature of any party in the supply chain (and pick the receiver accordingly).

In order to produce a signature the attacker must either obtain one of the private keys relating to a supply chain entity or attempt to break the cryptographic scheme employed to create the signature (and thus obtain the key). The strength of public key cryptography is well known and the original keys are only held by the originating parties (e.g. manufacturer) and the supply chain controller and never transmitted over the communications network.

The attacker cannot employ a signature from another tag/product since the signed message contains the unique product code. Optionally the message may also contain the TID although caution must be employed in relying on the assumption that the TID cannot be cloned.

The only reasonable recourse left to the attacker is to clone the signature and product identifier (and if required TID) from a similar product. Both the genuine and counterfeit products can then be released into the supply chain. Since the signature is only valid at a limited number of potential receivers (usually one), such duplication can be caught and isolated early within the supply chain by maintaining a cache of received products and avoiding the requirement to report received product identifiers to a central authority.

B. Goods Removal

There is little any electronic scheme can do to prevent the removal of goods (due to theft or diversion outside the legitimate supply chain). The best that any scheme can do is to

detect such activity and pinpoint where it occurs. None of the schemes we have considered (TRS, TRA, RP) will detect by themselves the removal of goods, since there is no expectation that goods should have been received (as there might be within a central track and trace system). If such attacks need to be considered then our design might be extended with a polling mechanism from the shipper to receiver or by pushing shipping information to the receiver. The problem with this in our current design is that the shipper does not necessarily know the identity of the receiver (if for example there are several intermediate parties which are not participating in the scheme). Such information may be divulged by the supply chain controller to the shipper, although this will result in some small amount of downstream visibility being released to the shipper contrary to our original design goals.

C. *Goods Substitution*

The attacker may substitute goods within the supply path. This can be performed by removing the tag from the genuine goods and transferring it to the goods being introduced. Alternatively the tag may be cloned and the genuine goods removed permanently from the authorised supply path. Ultimately no electronic scheme can prevent the transfer of tags and physical security should be considered (such as embedding the tags). The use of the TID within the signed message may hinder the cloning of the tag. If possible the value of any removed goods should be degraded to the point where such attacks are not economic (which occurs when the value of the removed goods is equal to the value of the counterfeit goods plus the cost of the attack). This can be achieved by limiting the end sale opportunities of unverified products. If none of these courses of action are sufficient then tags with cryptographic authentication abilities may be employed (although this obviously breaks our design goal of using basic insecure tags).

D. *Disruption of the Scheme*

Although we have considered how the scheme protects against supply chain attacks, we should also consider how the scheme may be disrupted by a malicious party that wants to cause damage to the legitimate supply chain partners. The scheme presented does not use any write protection for the tag signature. Therefore, any party may delete or change the signature. This would cause genuine goods that have traversed an authorised path to be rejected, resulting in expensive investigation. Widespread attacks can obviate the usefulness of the scheme. Attacks of this nature will be mitigated by the fact that the goods will have followed an authorised supply path, so access to malicious parties may be limited. If such threats are considerable then our scheme may be layered with additional tag security such as passwords or cryptographic-based access control.

VIII. DISCUSSION

In section III we stated our design goals were:

A) Limited supply chain visibility
B) No central run-time authority
C) Applicable to cheap insecure tags
D) Supply chain control instead of anti-counterfeiting

Our design prevents the dissemination of supply chain operational data to downstream parties (or other eavesdroppers). Only the receiver for the immediate upstream leg need know about shippers from whom they are allowed to receive certain goods. This information is in two parts. Firstly, upon receiving goods they can tell which authorised upstream shipper has supplied the goods. Secondly, in advance of receiving the goods they are provided with shipper information in the form of supply chain policies and public keys. In an ePedigree scheme where signatures are appended and checked only at the conclusion of the supply chain, this policy information would not be visible to intermediate supply chain partners. In our system this information is fragmented and distributed along the receivers in the supply path, limiting the abuse that any single party can perform with such information. In particular each receiver is likely to learn about shippers with whom they already have a close supply chain relationship.

Although not presented in our design it is important to realize that each receiver actually only knows about the public key of shippers for the immediate upstream segment. This is not the same as the identity of the shipper. Since the supply chain controller is responsible for the generation and distribution of such keys, it may allocate many keys to each shipper and routinely rotate these keys. In effect, each key does not identify the shipper, but only a temporary supply chain path segment.

In the proxy re-signature scheme the use of central authorities is kept to a minimum. We have achieved our goal of not referring to such authorities during the normal operation of the supply chain. Hence such authorities may not learn about the detailed flow of goods, even if they are the original manufacturer of the goods. If such authorities are unavailable, this will not impact on the performance of the routine operations and goods may continue to be processed. The long term unavailability of such authorities will only impede the updating of the permitted supply chain paths (which is likely to be performed well in advance of the flow of goods) and the reporting of violations.

We believe that our scheme is more suitable to cheap insecure tags that other signature-based schemes. Trivially it only requires enough tag memory for one signature (although we acknowledge that multi-signature schemes can also achieve this) and does not require write-once memory. In discussing the cloning of a tag we should consider (i) how easy it is to clone the tag and (ii) the damage that may be caused. In the system presented above the signature is created over the unique item identifier (to prevent the signature being used for other goods) and optionally the TID (to stop the signature being used on a tag with a different TID). In this respect it is similar to any other tag signature scheme. Many tags provide the ability to use reserved memory with access passwords. In our scheme such passwords would need to be shared between

all participants making them inherently weak. Also the use of item-level passwords would break our design goal of not using any central system. In this respect a scheme that appends signatures into write-once memory with a read password may have an advantage since the password need only be shared with the final verifier at the end of the supply chain. Strong protection against cloning may be gained by using cryptographic authentication-capable tags, although ideally the tag would need to be checked at each receiver to pinpoint any introduction of cloned tags. In any case, this approach breaks both of our goals of avoiding run-time communications with central authorities and not using specialist security tags. Tags capable of asymmetric cryptography could participate off-line in the signature creation. However, the public key would still need to be obtained on-line during the path segment verification process so little is gained over the use of symmetric cryptography.

Although our scheme does not provide any new protection against the cloning of a tag, it does have some interesting properties concerning the ability of an attacker to re-introduce cloned tags back into the supply chain. Specifically, the goods need to be re-introduced on the same path segment from which they were cloned. Thus, local caching of product identifiers may be very effective at stopping and pinpointing duplicate items. Schemes that append signatures and perform supply chain verification checks only at the end of the delivery path would discover any duplication much later (potentially after the goods have entered the consumer market) and will lack the ability to pinpoint where goods were introduced. Such schemes would also require the centralized checking of duplicates since the cloned items may arrive at different retail points.

Finally, we have designed our scheme to be capable of preventing attacks beyond counterfeiting. The scheme provides general security against the introduction and substitution of goods, but also constrains the flow of goods for economic or quality reasons.

IX. CONCLUSIONS

We have presented an incremental improvement on current RFID security schemes that propose to carry signatures or other trace information on the RFID tags. In particular our scheme restricts the visibility of sensitive supply chain operations to just one upstream segment. Despite this limited visibility all partners in the supply chain can have confidence that the goods have followed a legitimate supply chain path from the manufacturer (or other party as desired). In addition the scheme allows multiple supply chain authorities (e.g. manufacturers) to impose parallel restrictions over their shared distribution channels.

Although our scheme is based on RFID tag signatures, we still believe that cryptographic RFID tags and track and trace analytics both have an important role. Cryptographic tags still provide the best assurance that a tag (and hence a product if employed correctly) is genuine without the deployment of infrastructure throughout the supply chain partners. Meanwhile track and trace solutions can offer many advantages beyond controlling the introduction and diversion of goods. Such centralized solutions, for example, can learn expected behaviour and provide alerts during anomalous conditions [15]. They can also check complex conditional rules about the supply chain [17]. However, for many industries, the barriers to the central collection and processing of supply chain data will remain insurmountable. In these cases our scheme provides a method to control the supply chain path with minimal concerns over business confidentiality.

REFERENCES

[1] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. "Strong authentication for RFID systems using the AES algorithm", in Cryptographic Hardware and Embedded Systems, CHES, 2004

[2] P. Tuyls, L. Batina. "RFID-Tags for Anti-counterfeiting", in Topics in Cryptology, CT-RSA 2006

[3] D. Hein, J. Wolkerstorfer & N. Felber. "ECC is Ready for RFID –- A Proof in Silicon", Workshop on RFID Security 2008 (RFIDsec08), July 2008

[4] H. Bock, M. Braun, M. Dichtl, E. Hess, J. Heyszl, W. Kargl, H. Koroschetz, B. Meyer & H. Seuschek. "A Milestone Towards RFID Products Offering Asymmetric Authentication Based on Elliptic Curve Cryptography"., Invited talk at RFIDsec 2008, July 2008

[5] T. Staake, F. Thiesse & E.Fleisch. "Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting", ACM Symposium on Applied Computing, 2005.

[6] D. Molnar, A. Soppera & D. Wagner. "Privacy fro RFID Through Trusted Computing", in Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society, Alexandria, USA, 2005

[7] A. Soppera, T. Burbridge & V. Broekhuizen. "Trusted RFID Readers for Secure Multi-Party Services", EU RFID Forum 2007, Brussels, March 2007.

[8] T. Burbridge, A.Soppera, J. Farr, M. Lehtonen & A. Ilic. "Using the Trusted Reader for Product Authentication", BRIDGE project Deliverable D4.2.2B, www.bridge-project.eu, 2009.

[9] L. Harn & J Ren. "Efficient Identity-Based RSA Multisignatures", in Journal of Computers & Security 27, 2008.

[10] M. Lehtonen, A. Ruhanen, F. Michahelles & E. Fleisch. "Serialized TID Numbers – A Headache or a Blessing for RFID Crackers?", in IEEE International Conference on RFID, Orlando, 2009.

[11] http://www.trustedcomputinggroup.org/

[12] M. Blaze, G. Bleumer, and M. Strauss. "Divertible protocols and atomic proxy cryptography", in Advances in Cryptology, EUROCRYPT '98, 1998

[13] G. Ateniese and S. Hohenberger, "Proxy Re-Signatures: New Definitions, Algorithms, and Applications", in Proceedings of the 12th ACM conference on Computer and Communications Security, CCS, Alexandria, USA, November 2005

[14] B. Libert & D. Vergnaud, "Multi-use unidirectional proxy re-signatures", in Proceedings of the 15th ACM conference on Computer and Communications Security, CCS, Alexandria, USA, 2008

[15] EPCglobal Tag Data Standard (TDS). http://www.epcglobalinc.org/standards/tds/

[16] M. Harrison (editor) et al., "Serial-Level Inventory Tracking Model", BRIDGE project deliverable D3.1, www.bridge-project.eu, 2007.

[17] J. Al-Kassab, M. Lehtonen, F. Michahelles. "Anti-Counterfeiting Prototype Report", BRIDGE project deliverable D5.3, www.bridge-project.eu, 2008.